TECH TIP — BEGINNER

How to Set Up SSH on Linux

(The Easy One — It's Four Commands)

From Nolan Law Firm — nemolegal.com/tools

Linux Gets This Right

Setting up SSH on Linux takes about three minutes. It was designed to work this way. The Windows guide exists because Microsoft made a simple thing complicated. Linux didn't. This guide covers Ubuntu and Debian-based systems — which is most of what you'll encounter.

Step 1 — Install the SSH Server

Open a terminal and run:

```
sudo apt update && sudo apt install openssh-server -y
```

That's the whole installation. The `-y` flag just answers yes automatically so you don't have to confirm. Takes about 30 seconds.

Step 2 — Verify It's Running

```
sudo systemctl status ssh
```

You want to see **active (running)** in green. If it's not running, start it:

```
sudo systemctl start ssh

sudo systemctl enable ssh
```

The second command makes it start automatically on reboot. Run both just to be safe.

Step 3 — Open the Firewall

If you're running UFW (Ubuntu's firewall — you should be):

```
sudo ufw allow ssh

sudo ufw status
```

The status command shows what's allowed. SSH should appear in the list.

Step 4 — Find Your IP Address

```
ip a
```

Look for your network adapter (usually `eth0` for wired or `wlan0` for wireless) and find the `inet` line. That's your local IP — something like 192.168.1.112.

Step 5 — Connect From Another Machine

From any other computer on the same network:

```
ssh your-username@192.168.1.112
```

Replace `your-username` with your actual Linux username and the IP with yours. It will ask for your password. Type it. Done — you're in.

> **Tip:** Linux doesn't show characters when you type passwords. The cursor won't move. That's normal. Type your password and press Enter.

Bonus — Stop Typing Passwords (Key-Based Auth)

This is how professionals do it. Generate a key pair on the machine you're connecting *from*, then copy the public key to the Linux machine. After that, no password needed.

On the machine you're connecting from:

```
ssh-keygen -t ed25519

ssh-copy-id your-username@192.168.1.112
```

`ssh-keygen` creates your key pair. Just press Enter through the prompts the first time. `ssh-copy-id` installs your public key on the remote machine. After that, `ssh username@ip` connects instantly — no password.

Quick Reference

Task	Command
Install SSH server	`sudo apt install openssh-server -y`
Check status	`sudo systemctl status ssh`
Start SSH	`sudo systemctl start ssh`
Enable on boot	`sudo systemctl enable ssh`

Open firewall	`sudo ufw allow ssh`
Find your IP	`ip a`
Connect from another machine	`ssh username@ip-address`
Set up key auth (no password)	`ssh-keygen then ssh-copy-id username@ip`